(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 September 2001 (07.09.2001)

PCT

(10) International Publication Number
WO 01/65762 A2

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/US01/06911

(22) International Filing Date: 2 March 2001 (02.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/186,551 2 March 2000 (02.03.2000) US

(71) Applicant *(for all designated States except US)*: **TIVO, INC.** [US/US]; 2160 Gold Street, P.O. Box 2160, Aviso, CA 95002-2160 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **PLATT, David, C.** [US/US]; 323 Aldean Avenue, Mountain View, CA 94043 (US). **GOODMAN, Andrew** [US/US]; 2171 Avy Avenue, Menlo Park, CA 94025 (US). **ZENCHELSKY, Daniel** [US/US]; 497 San Benito Avenue, Los Gatos, CA 95030 (US).

(74) Agents: **GLENN, Michael** et al.; Glenn Patent Group, Suite L, 3475 Edison Way, Menlo Park, CA 94025 (US).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/65762 A2

(54) Title: CONDITIONAL ACCESS SYSTEM AND METHOD FOR PREVENTION OF REPLAY ATTACKS

(57) Abstract: In a conditional access system, a headend transmits content to one or more receivers in encrypted transport streams. The system provides a multi-layer security architecture, rendering the system resistant to key replay attacks; if one layer is circumvented, subsequent layers remain intact. A first layer prevents unencrypted keys from being recorded by shielding the unencrypted keys from users and encrypting the path from the receiver's conditional access module to the transport decryption module; a second layer prevents a key recorded on one receiver from being played back to the transport decryption module on a second receiver; a third layer prevents a user from decrypting transport streams without the encryption module by encrypting the stream a second time prior to being passed through any user-accessible memory or processor. Events tables are transmitted with the transport stream, either unencrypted for immediate use or encrypted, to prevent unauthorized use.

CONDITIONAL ACCESS SYSTEM AND METHOD FOR PREVENTION OF REPLAY ATTACKS

BACKGROUND OF THE INVENTION

TECHNICAL FIELD

The invention relates to security in conditional access systems. More particularly the invention relates to a conditional access system that includes a multi-layer cryptographic security architecture for prevention of replay attacks.

TECHNICAL BACKGROUND

In conditional access systems, such as cable television networks, audio, video, data and other forms of content in electronic form may be broadcast as digital transport streams. The transport stream originates at the system headend and is transmitted to and received by receiver units that display or make use of the transport stream. In order to prevent unauthorized use or viewing of the transport stream, the stream may be encrypted. In such systems, the receiver is capable of decrypting the transport stream prior to viewing or using it.

Typically, the algorithm used to encrypt the transport stream is controlled by an encryption key. When decrypting the transport stream at the receiver end, the receiver must have the key. As a security measure, the key is periodically changed. Because the key is changed on a regular basis, there can be multiple keys required to decrypt the transport stream. The keys are then encrypted and broadcast within the transport stream.

Generally, within the receiver unit of a conditional access system, a Transport Reception Module (TRM) is operative to receive the transport stream transmitted from the headend. Furthermore, a Conditional Access Module (CAM) decides whether or not to decrypt the stream, based on services purchased by the user. If the CAM allows the user to view or otherwise use the transport stream, it decrypts the keys and provides them to the Transport Decryption Module (TDM) for use in decrypting the transport stream. Thus, the TDM is operative to decrypt the transport stream, using the

decrypted keys supplied by the CAM. Following decryption, the decrypted stream is displayed to the user on a display module.

Often, encrypted transport streams are recorded by the receiver and stored for future use. Furthermore, current conditional access systems are subject to replay attacks, particularly key replay attacks, in which unencrypted decryption information is intercepted and recorded as it is being passed to a TDM. Subsequently, the recorded decryption information may then be used at a later time to gain unauthorized access to the encrypted transport streams. For example, User A and User B both record a transport stream containing a particular audio/video stream, such as a movie. User A purchases the service; therefore the CAM in A's receiver will provide keys to use in decrypting the transport stream. User A can record the keys provided by the CAM as they are being passed to the TDM, and send them to User B. Thus, User B is able to decrypt the stream using the keys provided by A, viewing or using the stream without purchasing it.

A. Wasilewski, H. Pinder, G. Akins, M. Palgon, *Conditional access system*, U.S. Patent No. 6,157,719 (December 5, 2000) and R. Banker, G. Akins, *Preventing replay attacks on digital information distributed by network service providers*, U.S. Patent No 6,005,938 (December 21,1999) provide techniques for preventing replay attacks on digital information distributed by network services. At the beginning of a subscription period for a service, a network service provider sends entitlement messages to the subscriber that provide the subscriber with a session key and authorization information, specifying a service and a period of time. When an encrypted service instance is distributed, it is accompanied by entitled control messages. The subscriber equipment that decrypts the service instance does so only if the time specifier in the entitlement control message specifies a time period specified by the authorization information. While the disclosed technique certainly complicates replay attacks by introducing a time element absent in conventional methods, it does not prevent them. In particular, it does not prevent recording and replaying of generated control words or instance keys.

S. Ooi, *Decryptor*, U.S. Patent No. 5,790,666 (August 4, 1998) describes a decryptor within a receiver unit of a conditional access system that includes a descrambler for descrambling signals scrambled at the headend using a pseudo-random noise generator. At the receiver, a pseudo-random noise generator is induced to change its state, through the provision of a scramble key, so that it generates pseudo-random noise signals that descramble the scrambled signal. The encrypted scramble key is transmitted from the headend and decrypted at the receiver after a cascade of conditions is satisfied. The decryptor, as described, provides a robust, multi-layer security apparatus for a conditional access system. Nevertheless, it suffers a vulnerability to

replay attacks common to many conditional access systems. The scramble key, when it has been decrypted, may be intercepted and recorded as it is passed to the descrambler. Subsequently, the recorded key may be replayed, either on the same receiver, or different receivers, creating the possibility of pirating and unauthorized use of the signal.

Accordingly, there exists a need for a way of preventing replay attacks in conditional access systems. It would be desirable to provide protection in multiple layers, so that if one layer is compromised, the other layers remain intact.

SUMMARY OF THE INVENTION

In a conditional access system, a headend transmits content to one or more receivers as encrypted transport streams. The system includes a multi-layer security architecture that renders the system highly resistant to key replay attacks at the receiver. Thus, if one layer is circumvented, the other layers remain intact. A first layer prevents unencrypted keys from being recorded by shielding the unencrypted keys from users and encrypting the path from the receiver's conditional access module (CAM) to the transport decryption module (TDM); a second layer prevents a key recorded on one receiver from being played back to the transport decryption module on a second receiver; and a third layer prevents a user from decrypting transport streams without the encryption module by encrypting the stream a second time prior to being passed through any user-accessible memory or processor.

The multi-layer security architecture is achieved by means of a series of cryptographic procedures between the headend and the various components of the receiver. First is a procedure for pairing the transport components with the CAM in which a random secret generated at the headend is encrypted and transmitted to the transport reception module (TRM), the TDM and the CAM. Each of the three components decrypts the secret and stores it for future use. Second is a transport stream recording procedure that requires a local key, specific to the receiver, generated by the CAM. Third is a procedure for decrypting and replaying the transport stream, also requiring the local key.

An event table for an MPEG stream is constructed in advance of the user purchasing rights to use the stream. In one embodiment, the event table is transmitted unencrypted, along with the corresponding stream, so that the receiver may access the

table without decrypting the stream. In an alternative embodiment, the event table is encrypted to prevent unauthorized use.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 provides a block diagram of a conditional access system that is resistant to replay attacks, according to the invention.

DETAILED DESCRIPTION

The invention provides a conditional access system that is resistant to playback attacks. The invention is also embodied as a cryptographic method for rendering a conditional access system resistant to replay attacks, particularly key replay attacks.

Referring now to Figure 1, shown is a conditional access system that includes a headend 11 and a receiver 12. In actual fact, the system includes a plurality of substantially identical receivers, but the invention is described herein in terms of one receiver. The receiver includes a transport reception module (TRM) 15 for receiving a transport stream 14 from the headend, and saving it to storage component 17. As Figure 1 shows, the transport stream 14 is encrypted by an encryptor 20 prior to transmission. Further, the receiver includes a transport decryption module (TDM) 16 that retrieves the transport stream from storage components 17 and decrypts it when access rights to the steam have been purchased by an end user. Additionally, the receiver includes a conditional access module (CAM) 18 that is operative to decide whether or not to decrypt the stream, based on the serves that the user has purchased. If the CAM allows the user to view or use the transport stream, it decrypts the key required to decrypt the transport stream and provides them to the TDM. The conditional access system 10 incorporates a multi-layer security architecture that prevents key replay attacks at the receiver 12. The novel security architecture relies on conventional encryption technology, applied in a new and unique way. The multi-layer security architecture, based on public key encryption is implemented in a series of cryptographic procedures, described in greater detail below.

By providing multiple layers of security, if one security layer is circumvented, the other layers remain intact, thus providing a much higher degree of protection against replay attacks than is conventionally possible.

A first security layer is provided to prevent keys from being recorded from the CAM 18. This is accomplished by never exposing unencrypted keys to the end user or any user programmable processor within the system, or storing them within any user-accessible memory within the system. Furthermore, the communication path between the CAM and the TDM is encrypted.

If, for some reason, the first layer were to fail, and the user were to gain access to the keys, a second layer prevents the keys from being played back to a TDM on another receiver by ensuring that the TDM will not accept the key without it being transformed in a way that is unique to a particular receiver. Thus, a local key is required that is derived from the decryption key provided by the headend. In the current invention, the CAM provides the functionality required to generate local keys. It should be noted that the degree of security provided by this layer is in direct proportion to the degree of difficulty a cracker would encounter in transforming one receiver's key into a key required by a second receiver.

A third layer of security prevents a user from intercepting the transport stream and decrypting it without the TDM. This is accomplished by never exposing the transport stream to the user. Before passing the stream through any user-programmable processor or user-accessible memory, the transport stream must be encrypted a second time. The security of the doubly-encrypted stream is further enhanced by providing an encryption mechanism that produces an encrypted stream that is particular to the receiver, rendering it useless on another receiver.

IMPLEMENTATION

The multi-layer security architecture is implemented as a series of cryptographic procedures, described in detail in Tables 1 – 3, below.

As shown in Figure 1,

The headend 11 has:

- a Global Secret Key: GSK;
- a Headend Private Key;
- receiver's Transport Public Key; and
- Receiver's CAM Public Key.

The TRM 15 has:

- Transport Private Key; and
- Headend Public Key.

Likewise, the TDM 16 also has:

- Transport Private Key; and

- Headend Public Key

The CAM 18 has:

- CAM Private Key;
- Headend Public Key;
- Global Secret Key; and
- CAM Secret Key.

Table 1: CAM to TRM/TDM Pairing Procedure

1. Headend generates random secret: S
2. Headend cryptographically signs S using Headend Public Key: HPK(S).
3. Headend encrypts S,HPK(S) using Transport Public Key: TPK(S,HPK(S)).
4. Headend encrypts S,HPK(S) using CAM Public Key: CPK(S,HPK(S)).
5. Headend transmits (TPK(S,HPK(S)) and CPK(S,HPK(S)) to TRM.
6. TRM decrypts TPK(S,HPK(S)) using Transport Private Key; S,HPK(S).
7. TRM verifies signature of HPK(S) using Headend Public Key. If signature is invalid, processing stops here.
8. TRM stores shared secret, S, for later use.
9. TRM passes TPK(S,HPK(S)) to TDM.
10. TDM decrypts TPK(S,HPK(S)) using Transport Private Key; S,HPK(S).
11. TDM verifies signature of HPK(S) using Headend Public Key. If signature is invalid, processing stops here.
12. TDM store shared secret, S, for future use.
13. TRM passes CPK(S,HPK(S)) to CAM.
14. CAM decrypts CPK(S,HPK(S)) using CAM Private Key: S,HPK(S).
15. CAM verifies signature of HPK(S) using Headend Public Key. If signature is invalid, processing stops here.
16. CAM stores shared secret, S, for future use.

Thus, as described in Table 1, above, a random secret is generated by the headend. As Figure 1 shows, the random secret is generated at the headend 11 by a pseudo-random number generator 19. However, other equally suitable methods of generating the secret will be apparent to those skilled in the art. The general direction of the encrypted signal is shown by arrow 13. Thus, encrypted decryption keys, encrypted, signed secrets, and the encrypted transport stream itself traverse this same path from the headend to the receiver. The encrypted keys and secrets may be provided at the same time as the transport stream, either embedded in the stream, or as a separate stream, or they may be provided separately from the transport stream. Upon being received from the headend, the TRM, the TDM and the CAM all receive the encrypted secret. They decrypt the secret, verify the signature and store the secret for future use. As described below, the shared secret is necessary for the generation and utilization of the local key, which is required for recording and decrypting the transport stream.

Table 2: Transport Stream Recording Procedure

1. Headend generates an encryption Key: K.
2. Headend encrypts key using Global Secret Key: GSK(K).
3. Headend transmits GSK(K) to TRM.

4. Headend encrypts transport stream using K: K(TS).
5. TRM sends GSK(K) to CAM.
6. CAM generates Local Key by encrypting GSK(K) using CAM Secret Key: LK=CSK(GSK(K)).
7. CAM encrypts LK using shared secret, S: S(LK).
8. CAM sends S(LK) to TRM.
9. TRM decrypts S(LK) using shared secret, S: LK.
10. Headend transmits K(TS) to TRM.
11. TRM further encrypts K(TS) using LK: LK(K(TS)).
12. TRM stores GSK(K) and LK(K(TS)) on a storage medium.

As Table 2 describes, the encrypted decryption key is transmitted from the headend. The CAM transforms the decryption key using the CAM secret key, and the shared secret, S, both unique to that particular receiver, rendering the decryption key useless on any other receiver. The local secret is transmitted to the TRM from the CAM. Prior to being stored, in storage component 17, the encrypted transport stream is encrypted a second time, using the local key, effectively rendering the transport stream inaccessible. It should be mentioned that the storage component may consist of a memory or a mass storage device. The mass storage device may be a fixed drive such as a disk drive, or it may be a removable storage medium, such as a DVD.

Table 3: Transport Stream Playback Procedure

1. TDM retrieves GSK(K) and LK(K(TS)) from storage medium.
2. TDM sends GSK(K) to CAM
3. CAM generates Local Key by encrypting GSK(K) using CAM Secret Key: LK=CSK(GSK(K)).
4. CAM decrypts GSK(K) using GSK: K.
5. CAM encrypts K, LK using shared secret, S: S(K,LK).
6. CAM sends S(K,LK) to Transport.
7. TDM decrypts S(K,LK) using shared secret, S:K,LK.
8. TDM decrypts LK(K(TS)) using LK: K(TS).
9. TDM decrypts K(TS) using K: TS.
10. TDM sends Transport Stream, TS, to display module

As Table 3 describes, the TDM retrieves the doubly encrypted transport stream from the storage component 17, along with the decryption key. The decryption key is transmitted to the CAM, whereupon it is transformed into a local key, using shared secret, S and the CAM secret key. Prior to display, the transport stream must be decrypted twice. The first time using the local key, and the second time using the decryption key provided by the headend. Thus, in the form it is retrieved from the storage component, the transport stream is useless, except on that particular receiver.

The invention is applicable in any type of subscription-based or conditional access network environment, in which a network service provider distributes digital information to users of the network. Typically, the network will be a publicly-accessible

telecommunications network such as a cable television network or the Internet. Furthermore, the network connection may be wired or wireless. Depending on the network and the nature of the content provided, the receiver may constitute a set-top box or a personal computer. The nature of the content is highly-variable; the invention is equally applicable to television programming, movies, pay-per-view sports events, digital music, digitized images, information products in digital format or software. Other network environments, hardware platforms and areas of application consistent with the spirit and scope of the invention will be apparent to those skilled in the art.

* * * * *

MPEG is an industry standard for compressing, multiplexing, and transmitting digital video and audio. An MPEG stream is composed of a sequence of data bytes. These bytes can be logically grouped together to form a single element within an MPEG stream. For example, a single element within an MPEG stream might represent a single frame of video within a movie.

The MPEG standard defines byte sequences that indicate the start of an element within an MPEG stream; such byte sequences are commonly referred to as "start codes." Some common examples of MPEG start codes are:

- Video Packetized Elementary Stream Header;
- Video Group of Pictures Header;
- Video I Frame Header;
- Video P Frame Header;
- Video B Frame Header;
- Video Slice Header; and
- Audio Packetized Elementary Stream Header.

It is often useful or necessary to build an Event Table that indicates the location of start codes within an MPEG stream. This table is composed of a list of offsets into the MPEG stream. The offsets listed in the table correspond to location in the MPEG stream that contain start codes.

The Event table may contain additional information, as well. For example, it is often useful to describe what type of start code is located at each offset. Using the Event Table allows a playback device to quickly locate a particular element within an MPEG stream. For example, one method of quickly scanning through video (fast forward) is to play only a subset of the video frames contained within the stream. The Event Table can be used to quickly locate those frames that need to be displayed.

One application where it is useful to build such a table is on a device designed to receive, store and play back MPEG stream transmissions. Since MPEG streams are often encrypted before transmission to prevent unauthorized use, it is desirable to store the MPEG stream at the receiver in its encrypted from prior to purchase, in order to prevent unauthorized use. Typically, the stream is not decrypted until the rights to use or view the stream are purchased. Conventionally, the event table cannot be built until the MPEG stream is decrypted. Building the event table can be a time consuming process. Accordingly, this can impose a significant time delay between the time that the rights to use the stream are purchased and the time that the Event Table is created and available for use.

In order to make the Event Table available immediately, an embodiment of the invention is provided in which the Event Table is created prior to transmission of the stream. A first alternative is to transmit the Event Table along with the associated MPEG stream, so that the receiver has access to the Event Table without decrypting the MPEG stream. A second alternative is to encrypt the Event Table itself prior to transmission, to protect it from unauthorized use.

Although the invention has been described herein with reference to certain preferred embodiments, one skilled in the art will readily appreciate that other applications may be substituted without departing from the spirit and scope of the present invention. Accordingly, the invention should only be limited by the Claims included below.

CLAIMS

What is claimed is:

1. A cryptographic method for rendering a conditional access system resistant to playback attacks, said system comprising a headend and at least one receiver connected to said headend, said method comprising the steps of:

providing at least a global secret key (GSK), headend public (HPK) and private keys, receiver transport public (TPK) and private keys; receiver conditional access module (CAM) public (CPK) and private keys and a CAM secret key (CSK);

pairing transport reception and decryption components of the receiver with said CAM such that a Transport Reception Module (TRM), a Transport Decryption Module TDM) and said CAM all share a secret;

generating a Local Key (LK);

recording an encrypted transport stream transmitted from said headend, wherein the transport stream is further encrypted at said receiver, using LK, so that a doubly-encrypted transport stream is stored on a storage medium on said receiver; and

playing back said transport stream, wherein said transport stream is decrypted by said TDM, using LK.

2. The method of Claim 1, wherein said step of pairing transport reception and decryption components of the receiver with said CAM comprises the steps of:

generating a random secret (S) by said headend;

signing S by said headend using HPK (HPK(S));

encrypting S, HPK(S) by said headend using TPK (TPK(S, HPK(S));

encrypting S, HPK(S) by said headend using CPK (CPK(S, HPK(S));

transmitting TPK(S, HPK(S) and CPK(S, HPK(S) to TRM by said headend;

decrypting TPK(S, HPK(S) by TRM using said Transport private key;

verifying said signature (HPK(S) by TRM using HPK, wherein processing stops if said signature is invalid;

storing S for future use by TRM;

passing TPK(S, HPK(S) to TDM by TRM;

decrypting TPK(S, HPK(S) by TDM using said Transport private key;

verifying said signature (HPK(S) by TDM using HPK, wherein processing stops if said signature is invalid;

storing S for future use by TDM;
passing CPK(S, HPK(S) to CAM by TRM;
decrypting CPK(S, HPK(S) by CAM using said CAM private key;
verifying said signature (HPK(S) by CAM using HPK, wherein processing stops if said signature is invalid; and
storing S for future use by CAM;
wherein S is shared by TRM, TDM and CAM.

3. The method of Claim 2, wherein said step of recording an encrypted transport stream transmitted from said headend comprises the steps of:
generating an encryption key, K by said headend;
encrypting K using GSK (GSK(K));
transmitting GSK(K) to TRM;
encrypting a transport stream (TS) by said headend using K (K(TS));
sending GSK(K) to CAM by TRM;
generating LK, wherein generating LK comprises:
encrypting GSK(K) by CAM using CSK (LK=CSK(GSK(L)));
encrypting LK by CAM using S (S(LK));
sending S(LK) to TRM;
decrypting S(LK) by TRM using S
transmitting K(TS) to TRM by said headend;
further encrypting K(TS) using LK (LK(K(TS)); and
storing LK(K(TS) on said storage medium;
wherein said transport stream is doubly encrypted.

4. The method of Claim 3, wherein said step of playing back said transport stream comprises the steps of:
retrieving GSK(K) and LK(K(TS) by TDM;
sending GSK(K) to CAM by TDM;
generating LK by CAM;
decrypting GSK(K) by CAM suing GSK;
encrypting K, LK by CAM using S (S(K,LK));
sending S(K,LK) to TDM by CAM;
decrypting S(K, LK) by TDM using S;
decrypting LK(K(TS) by TDM using LK;
decrypting K(TS) by TDM using K; and
sending said decrypted transport stream TS to a display module for one of display and use by a user.

5. The method of Claim 4, wherein multiple layers of security are provided so that if one layer is a circumvented, subsequent layers remain intact.

6. The method of Claim 5, wherein a first layer comprises preventing said user from accessing unencrypted keys by avoiding exposing said unencrypted keys to user accessible and user programmable resources within said receiver.

7. The method of Claim 6, wherein said first layer further comprises encrypting a communication path between said CAM and said TDM.

8. The method of Claim 5, wherein a second layer comprises preventing keys from being played back into said TDM by requiring that keys be first transformed in a manner particular to a receiver.

9. The method of Claim 8, wherein said transformation comprises encrypting said keys by said CAM using LK.

10. The method of Claim 5, wherein a third layer comprises preventing said user from accessing said transport stream.

11. The method of Claim 10, wherein preventing said user from accessing said transport stream comprises doubly encrypting said transport stream prior to storage.

12. The method of Claim 11, wherein a corresponding Event Table is built for said transport stream prior to transmission.

13. The method of Claim 12, wherein said Event Table is transmitted along with said transport stream so that said Event Table is available for immediate use by said receiver.

14. The method of Claim 12, wherein said Event Table is encrypted prior to transmission to prevent unauthorized use.

15. A conditional access system rendered resistant to playback attacks, wherein multiple layers of security are provided so that if one layer is circumvented, subsequent layers remain intact, said system comprising:

a headend, wherein said headend sources a digital transport stream;

at least one receiver connected to said headend for receiving said transport stream, said receiver including a Transport Reception Module (TRM), a Transport Decryption Module (TDM) and a Conditional Access Module (CAM);

a global secret key (GSK);

headend public (HPK) and private keys;

receiver transport public (TPK) and private keys; and

receiver conditional access module (CAM) public (CPK) and private keys and a CAM secret key (CSK), wherein said keys are operative in a plurality of cryptographic procedures.

16. The system of Claim 15, wherein a first layer comprises preventing a user from accessing unencrypted keys by avoiding exposing said unencrypted keys to user accessible and user programmable resources within said receiver.

17. The system of Claim 16, wherein said first layer further comprises encrypting a communication path between said CAM and said TDM.

18. The system of Claim 16, wherein a second layer comprises preventing keys from being played back into said TDM by requiring that keys be first transformed in a manner particular to a receiver.

19. The system of Claim 18, wherein said transformation comprises encrypting said keys by said CAM using a local key (LK) generated by said CAM.

20. The system of Claim 19, wherein a third layer comprises preventing said user from accessing said transport stream.

21. The system of Claim 20, wherein preventing said user from accessing said transport stream comprises doubly encrypting said transport stream prior to storing said transport stream locally.

22. The system of Claim 21, wherein transport reception and decryption components of the receiver are paired with said CAM such that said TRM, said TDM and said CAM all share a secret, and wherein said pairing is accomplished by:

generating a random secret (S) by said headend;

signing S by said headend using HPK (HPK(S));

encrypting S, HPK(S) by said headend using TPK (TPK(S, HPK(S));

encrypting S, HPK(S) by said headend using CPK (CPK(S, HPK(S));

transmitting TPK(S, HPK(S) and CPK(S, HPK(S) to TRM by said headend;

decrypting TPK(S, HPK(S) by TRM using said Transport private key;

verifying said signature (HPK(S) by TRM using HPK, wherein processing stops if said signature is invalid;

storing S for future use by TRM;

passing TPK(S, HPK(S) to TDM by TRM;

decrypting TPK(S, HPK(S) by TDM using said Transport private key;

verifying said signature (HPK(S) by TDM using HPK, wherein processing stops if said signature is invalid;

storing S for future use by TDM;

passing CPK(S, HPK(S) to CAM by TRM;

decrypting CPK(S, HPK(S) by CAM using said CAM private key;

verifying said signature (HPK(S) by CAM using HPK, wherein processing stops if said signature is invalid; and

storing S for future use by CAM;

wherein S is shared by TRM, TDM and CAM.

23. The system of Claim 22, wherein an encrypted transport stream transmitted from said headend is recorded, wherein the transport stream is further encrypted at said receiver, using LK, so that a doubly-encrypted transport stream is stored on a storage medium on said receiver;

wherein recording said stream comprises:

generating an encryption key, K by said headend;

encrypting K using GSK (GSK(K));

transmitting GSK(K) to TRM;

encrypting a transport stream (TS) by said headend using K (K(TS));

sending GSK(K) to CAM by TRM;

generating LK, wherein generating LK comprises:

encrypting GSK(K) by CAM using CSK (LK=CSK(GSK(L)));

encrypting LK by CAM using S (S(LK));

sending S(LK) to TRM;

decrypting S(LK) by TRM using S

transmitting K(TS) to TRM by said headend;

further encrypting K(TS) using LK (LK(K(TS)); and

storing LK(K(TS) on said storage medium;

wherein said transport stream is doubly encrypted.

playing back said transport stream, wherein said transport stream is decrypted by said TDM, using LK.

24. The system of Claim 23, wherein said transport stream is decrypted by said TDM, using LK and played back by:

retrieving GSK(K) and LK(K(TS) by TDM;

sending GSK(K) to CAM by TDM;

generating LK by CAM;

decrypting GSK(K) by CAM suing GSK;

encrypting K, LK by CAM using S (S(K,LK));

sending S(K,LK) to TDM by CAM;

decrypting S(K, LK) by TDM using S;

decrypting LK(K(TS) by TDM using LK;

decrypting K(TS) by TDM using K; and

sending said decrypted transport stream TS to a display module for one of display and use by said user.

25. The system of Claim 15, further comprising a corresponding event table for said transport stream, wherein said event table is built prior to transmission.

26. The system of Claim 25, wherein said Event Table is transmitted along with said transport stream so that said Event Table is available for immediate use by said receiver.

27. The system of Claim 25, wherein said Event Table is encrypted prior to transmission to prevent unauthorized use.

28. A method of providing an event table for a corresponding MPEG transport stream, wherein said transport stream is transmitted from a headend to at least one receiver, said method comprising;

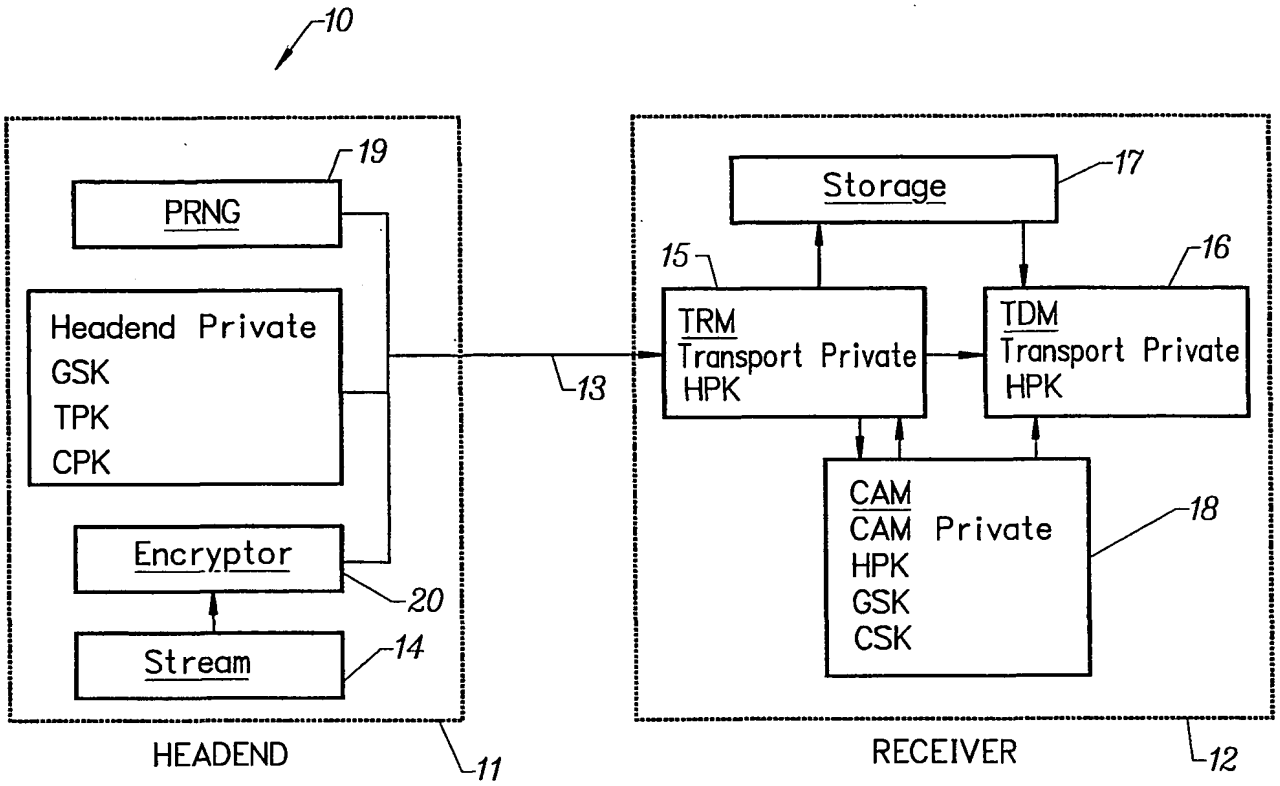
building said event table prior to transmission of said stream.

29 The method of Claim 28, further comprising the step of:

transmitting said event table along with said transport stream so that said event table is available for immediate use by said receiver.

30. The method of Claim 29, further comprising the step of:

encrypting said event table prior to transmission so that unauthorized use of said event table is prevented.



Legend

CAM	Conditional Access Module
TRM	Transport Reception Module
TDM	Transport Decryption Module
GSK	Global Secret Key
TPK	Transport Public Key
CPK	CAM Public Key
HPK	Headend Public Key
CSK	CAM Secret Key

FIG. 1

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 September 2001 (07.09.2001)

PCT

(10) International Publication Number
WO 01/65762 A3

(51) International Patent Classification[7]: H04N 7/167, 5/913, 5/00, H04L 9/08

(21) International Application Number: PCT/US01/06911

(22) International Filing Date: 2 March 2001 (02.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/186,551 2 March 2000 (02.03.2000) US

(71) Applicant *(for all designated States except US)*: **TIVO, INC.** [US/US]; 2160 Gold Street, P.O. Box 2160, Aviso, CA 95002-2160 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **PLATT, David, C.** [US/US]; 323 Aldean Avenue, Mountain View, CA 94043 (US). **GOODMAN, Andrew** [US/US]; 2171 Avy Avenue, Menlo Park, CA 94025 (US). **ZENCHELSKY, Daniel** [US/US]; 497 San Benito Avenue, Los Gatos, CA 95030 (US).

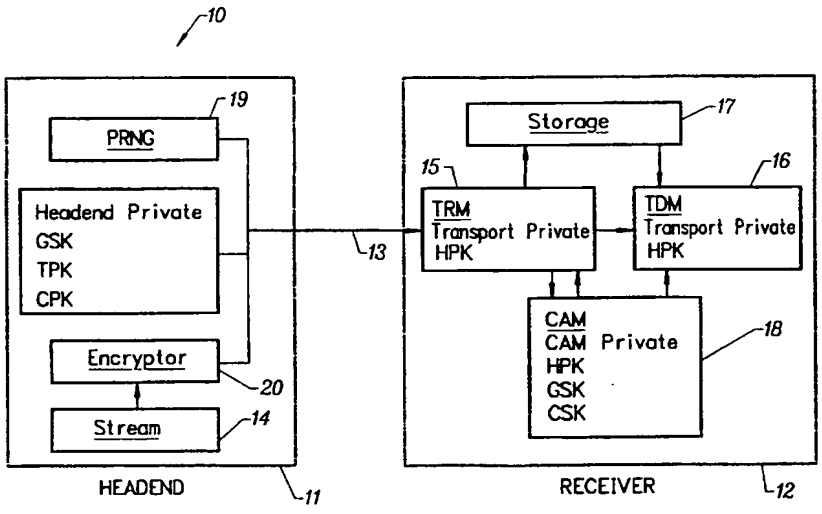
(74) Agents: **GLENN, Michael** et al.; Glenn Patent Group, Suite L, 3475 Edison Way, Menlo Park, CA 94025 (US).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,

[Continued on next page]

(54) Title: CONDITIONAL ACCESS SYSTEM AND METHOD FOR PREVENTION OF REPLAY ATTACKS



Legend

CAM	Conditional Access Module
TRM	Transport Reception Module
TDM	Transport Decryption Module
GSK	Global Secret Key
TPK	Transport Public Key
CPK	CAM Public Key
HPK	Headend Public Key
CSK	CAM Secret Key

(57) Abstract: In a conditional access system, a headend transmits content to one or more receivers in encrypted transport streams. The system provides a multi-layer security architecture, rendering the system resistant to key replay attacks; if one layer is circumvented, subsequent layers remain intact. A first layer prevents unencrypted keys from being recorded by shielding the unencrypted keys from users and encrypting the path from the receiver's conditional access module to the transport decryption module; a second layer prevents a key recorded on one receiver from being played back to the transport decryption module on a second receiver; a third layer prevents a user from decrypting transport streams without the encryption module by encrypting the stream a second time prior to being passed through any user-accessible memory or processor. Events tables are transmitted with the transport stream, either unencrypted for immediate use or encrypted, to prevent unauthorized use.

WO 01/65762 A3

IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
10 May 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INT NATIONAL SEARCH REPORT

Internal Application No
PCT/US 01/06911

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/167 H04N5/913 H04N5/00 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N H04L G11B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 991 400 A (KAMPERMAN FRANCISCUS L A J) 23 November 1999 (1999-11-23) abstract ---	1,15
A	US 5 862 299 A (GOTO KOICHI ET AL) 19 January 1999 (1999-01-19) abstract ---	1,15
A	WO 99 07145 A (SCIENTIFIC ATLANTA) 11 February 1999 (1999-02-11) abstract ---	1,15
A	EP 0 864 959 A (MITSUBISHI CORP) 16 September 1998 (1998-09-16) abstract -----	1,15

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 September 2001	05. 02. 2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	DOCKHORN H.S.

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 01/06911

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-27

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-27

   Conditional access system resistant to replay attacks

2. Claims: 28-30

   Provision of an event table for an MPEG stream

INT NATIONAL SEARCH REPORT

Information on patent family members

Interna... Application No
PCT/US 01/06911

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5991400 A	23-11-1999	EP 0800745 A1	15-10-1997
		WO 9716924 A1	09-05-1997
		JP 10512428 T	24-11-1998
US 5862299 A	19-01-1999	AU 3003597 A	07-01-1998
		EP 0906693 A1	07-04-1999
		JP 2000512824 T	26-09-2000
		WO 9749238 A1	24-12-1997
		US 6266481 B1	24-07-2001
		US 6104860 A	15-08-2000
WO 9907145 A	11-02-1999	US 6105134 A	15-08-2000
		AU 1581699 A	08-03-1999
		AU 8670598 A	22-02-1999
		AU 8679798 A	22-02-1999
		AU 8679898 A	22-02-1999
		AU 8764298 A	22-02-1999
		AU 8823398 A	22-02-1999
		AU 8823698 A	22-02-1999
		BR 9810966 A	20-11-2001
		BR 9810967 A	30-10-2001
		BR 9815606 A	22-01-2002
		BR 9815607 A	13-11-2001
		DE 69802288 D1	06-12-2001
		DE 69802540 D1	20-12-2001
		EP 1010323 A1	21-06-2000
		EP 1010324 A1	21-06-2000
		EP 1010325 A1	21-06-2000
		EP 1013091 A1	28-06-2000
		EP 1000508 A1	17-05-2000
		EP 1000509 A1	17-05-2000
		EP 1000511 A2	17-05-2000
		JP 2001513587 T	04-09-2001
		JP 2001512842 T	28-08-2001
		WO 9907145 A1	11-02-1999
		WO 9907146 A1	11-02-1999
		WO 9907147 A1	11-02-1999
		WO 9907148 A1	11-02-1999
		WO 9907149 A1	11-02-1999
		WO 9909743 A2	25-02-1999
		WO 9907150 A1	11-02-1999
		US 6292568 B1	18-09-2001
		US 6252964 B1	26-06-2001
		US 2001001014 A1	10-05-2001
		US 2001046299 A1	29-11-2001
		US 2001053226 A1	20-12-2001
EP 0864959 A	16-09-1998	JP 10254909 A	25-09-1998
		EP 0864959 A2	16-09-1998